AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A method in a data processing system for validating digital certificates having a server, an Online Certificate Status Protocol (OCSP) responder, and a certificate authority associating a certificate database including records associated with digital certificates, the method comprising:

receiving, at the OCSP responder, an OCSP request associated with a digital certificate generated by the server;

creating, by the OCSP responder, a Lightweight Directory Access Protocol database query based on the received OCSP request;

sending, by the OCSP responder, the Lightweight Directory Access Protocol database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid;

receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired";

determining, by the OCSP responder, the validity of the digital certificate based on the database query result; and

notifying the server of the determined validity of the digital certificate.

2. (Previously Presented) The method of claim 1, wherein the Lightweight Directory Access Protocol database query includes an instruction to return a selected portion of a database record.

3. (Previously Presented) The method of claim 1, wherein the method further comprises:

sending an indication of a new digital certificate from the certificate authority to the certificate database upon issuance of the new digital certificate;

receiving, by the certificate database, from the certificate authority, an indication of the new digital certificate; and

creating a certificate database record reflecting an identity of the new digital certificate.

4. (Previously Presented) The method of claim 1, wherein the method further comprises:

sending an indication of a revoked digital certificate from the certificate authority to the certificate database upon revocation of the revoked digital certificate;

receiving, by the certificate database, from the certificate authority, the indication of revocation of the revoked digital certificate; and

removing a certificate database record associated with the revoked digital certificate from the certificate database.

5. (Currently Amended) A method in a data processing system for validating digital certificates, the data processing system having a certificate authority and a directory server having a database, the method performed by the directory server comprising:

maintaining a database of valid digital certificates;

receiving a Lightweight Directory Access Protocol query based on an online certificate status protocol request indicating a requested digital certificate;

searching the database for a database record reflecting an identity of the requested digital certificate; and

returning an indication of the database record when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate, whereby the indication of the database record includes meta-data reflecting the validity of the requested digital certificate, permissible values of the meta data including at least "valid," "invalid," "revoked," "expired," and "revoked expired".

6. (Previously Presented) The method of claim 5, wherein maintaining a database further comprises:

sending an indication of a new digital certificate from the certificate authority to the database upon issuance of the new digital certificate by the certificate authority;

receiving, by the database from the certificate authority, an indication of the new digital certificate upon issuance of the new digital certificate by the certificate authority; and

storing a database record reflecting an identity of the new digital certificate.

7-11. (Canceled)

12. (Currently Amended) A method in a data processing system for validating digital certificates without certification revocation lists, the data processing system having a client, a server, a responder, a certificate authority associating a database storing records of valid digital certificates of the certificate authority, the method comprising:

generating, by the client, a request for a transaction, the request including a digital certificate identifying the client;

receiving the client request by the server;

creating, by the server, an online certificate status protocol request based on the associated digital certificate identifying the client;

sending, by the server, the online certificate status protocol request to the responder;

receiving, by the responder, the online certificate status protocol request associated with the digital certificate;

creating, by the responder, a Lightweight Directory Access Protocol database query based on the received online certificate status protocol request;

sending, by the responder, the Lightweight Directory Access Protocol database query to the database associated with the certificate authority to determine whether the digital certificate is valid;

searching the database for a database record identifying the digital certificate associated with the online certificate status protocol request, wherein the certificate database record stores a certificate and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired";

returning a LDAP database query result indicating whether the database record identifying the digital certificate is stored in the database;

sending, by the responder, a validity indication whether the digital certificate is valid based on the query result to the server; and

sending, by the server to the client, an indication of whether the transaction is authorized based on the validity indication.

13. (Currently Amended) A data processing system for answering online certificate status requests without certificate revocation lists, comprising:

a memory having program instructions;

a processor configured to execute the program instructions to:

receive from a server an online certificate status protocol request associated with a digital certificate,

create a Lightweight Directory Access Protocol database query based on the received request,

send the Lightweight Directory Access Protocol database query to a database associated with a certificate authority to determine whether the digital certificate is valid,

receive a Lightweight Directory Access Protocol database query result from the database indicating whether the digital certificate matches a corresponding entry stored in a database one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired",

determine the validity of the digital certificate based on the database query result, and

notify the server of the determined validity of the digital certificate.

14-15. (Canceled)

16. (Currently Amended) A data processing system for answering online certificate status requests without certificate revocation lists, comprising:

a client computer configured to send a request for a transaction, the request including a digital certificate identifying the client;

a server computer configured to receive the client request, create an online certificate status protocol request based on the associated digital certificate identifying the client, and send the online certificate status protocol request;

an OCSP responder configured to receive the online certificate status protocol request associated with the digital certificate, create a Lightweight Directory Access Protocol database query based on the received online certificate status protocol

request, and send the Lightweight Directory Access Protocol database query to determine whether the digital certificate is valid;

a certificate authority that provides valid digital certificates; and

a database associated with the certificate authority storing records of valid certificates of the certificate authority and configured to search for a database record identifying the digital certificate associated with the online certificate status protocol request, return an LDAP database query result indicating whether the digital certificate matches one of the records stored in the database, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired",

wherein the OCSP responder determines that the digital certificate is valid when it receives an LDAP database query result reflecting that the digital certificate matches one of the database records.

17. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for validating digital certificates, the data processing system having a server, an Online Certificate Status Protocol (OCSP) responder, a certificate authority associating a certificate database including records associated with digital certificates, the method comprising the steps of:

receiving, at the OCSP responder, an OCSP request associated with a digital certificate generated by the server;

creating, by the OCSP responder, a Lightweight Directory Access Protocol database query based on the received OCSP request;

sending, by the OCSP responder, the Lightweight Directory Access Protocol database query to the certificate database associated with the certificate authority to determine whether the digital certificate is valid;

receiving, at the OCSP responder, a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired";

determining, by the OCSP responder, the validity of the digital certificate based on the database query result; and

notifying the server of the determined validity of the digital certificate.

18. (Previously Presented) The computer-readable medium of claim 17, wherein the Lightweight Directory Access Protocol database query includes an instruction to return a selected portion of a database record.

19. (Previously Presented) The computer-readable medium of claim 17, wherein the method further comprises:

sending an indication of a new digital certificate from the certificate authority to the database upon issuance of the new digital certificate;

receiving, by the database, from the certificate authority, an indication of the new digital certificate; and

storing a database record reflecting an identity of the new digital certificate.

20. (Previously Presented) The computer-readable medium of claim 17, wherein the method further comprises:

sending an indication of a revoked digital certificate from the certificate authority to the database upon revocation of the revoked digital certificate;

receiving, by the database, from the certificate authority, the indication of revocation of the revoked digital certificate; and

removing a database record of an identity of the revoked digital certificate.

21. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for validating digital certificates, the data processing system having a certificate authority and a directory server having an associated database, the method performed by the directory server comprising:

maintaining a database of valid digital certificates;

receiving a Lightweight Directory Access Protocol query based on an online certificate status protocol request indicating a requested digital certificate;

searching the database for a database record reflecting an identity of the requested digital certificate; and

returning an indication of the database record when the database record reflecting the requested digital certificate is found to indicate validity of the requested digital certificate, whereby the indication of the database record includes meta-data reflecting the validity of the requested digital certificate, permissible values of the meta-data including at least "valid," "invalid," "revoked," "expired," and "revoked expired".

22. (Previously Presented) The computer-readable medium of claim 21, wherein maintaining a database further comprises:

sending an indication of a new digital certificate from the certificate authority to the database upon issuance of the new digital certificate;

receiving, by the database from the certificate authority, an indication of the new digital certificate upon issuance of the new digital certificate; and

storing a database record reflecting an identity of the new digital certificate.

23-27. (Canceled)

28. (Currently Amended) A computer-readable medium containing instructions for controlling a data processing system to perform a method for validating digital certificates without certification revocation lists, the data processing system having a client, a server, an responder, a certificate authority associating a database storing records of valid digital certificates of the certificate authority, the method comprising ~~the steps of~~:

generating, by the client, a request for a transaction, the request including a digital certificate identifying the client;

receiving the client request by the server;

creating, by the server, an online certificate status protocol request based on the associated digital certificate identifying the client;

sending, by the server, the online certificate status protocol request to the responder;

receiving, by the responder, the online certificate status protocol request associated with the digital certificate;

creating, by the responder, a Lightweight Directory Access Protocol database query based on the received online certificate status protocol request;

sending, by the responder, the Lightweight Directory Access Protocol database query to the database associated with the certificate authority to determine whether the digital certificate is valid;

searching the database for a database record identifying the digital certificate associated with the online certificate status protocol request, wherein the certificate database record stores a certificate and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired";

returning a LDAP database query result indicating whether the digital certificate the database record is stored in the database;

sending, by the responder, a validity indication whether the digital certificate is valid based on the query result to the server; and

sending, by the server to the client, an indication of whether the transaction is authorized based on the validity indication.

29. (Currently Amended) A data processing system for validating digital certificates, comprising:

means for receiving an OCSP request associated with a digital certificate generated by a server;

means for creating a Lightweight Directory Access Protocol database query based on the received OCSP request;

means for sending the Lightweight Directory Access Protocol database query to a certificate database associated with a certificate authority including records associated with digital certificates to determine whether the digital certificate is valid;

means for receiving a database query result indicating whether the digital certificate matches a corresponding certificate entry stored in one of the certificate database records, wherein the certificate database records store certificates and corresponding certificate information reflecting status of the certificate, permissible values of the certificate information including at least "valid," "invalid," "revoked," "expired," and "revoked expired";

means for determining the validity of the digital certificate based on the database query result; and

means for notifying the server of the determined validity of the digital certificate.

30. (Previously Presented) The method according to claim 1, wherein

the server and the OCSP responder reside in a first computer network,

the certificate authority and the certificate database reside in a second computer network, and

the first computer network is connected to the second computer network via a computer network firewall.